Cyber-diplomacy: the making of an international society in the digital age[1]

André Barrinha, University of Bath (UK) and Centre for Social Studies (Portugal), a.barrinha@bath.ac.uk
Thomas Renard, Egmont – Royal Institute for International Relations (Belgium), t.renard@egmontinstitute.be (corresponding author)

Abstract
Cyberspace has become a major locus and focus of international relations. Most global powers have now streamlined cyber issues into their foreign policies, adopting cyber strategies, and appointing designated diplomats to pursue these strategic objectives. This article proposes to explore the concept of cyber-diplomacy, by analysing its evolution and linking it to the broader discussions of diplomacy as a fundamental institution of international society, as defined by the English School of International Relations. It argues that cyber-diplomacy is an emerging international practice that is attempting to construct a cyber-international society, bridging the national interests of states with world society dynamics - the predominant realm in which cyberspace has evolved in the last four decades.

Keywords: diplomacy, Cybersecurity, cyber-diplomacy, international society, foreign policy

"By itself, the internet will not usher in a new era of international cooperation. That work is up to us." (Barack Obama, 2011)

Introduction

Cyber espionage, cyber-attacks, hacktivism, internet censorship and even supposedly technical issues such as net neutrality are now making the headlines on a regular basis. Cyberspace has become a contested political space, shaped by diverging interests, norms and values. As a result of this politicisation, diplomats have entered the game. If cyberspace was once a domain for technical discussions among IT specialists only, that era is definitively over.

The role of diplomacy in cyberspace is much less prominent in the media than stories of cyber incidents. A notable exception was the 2015 cybersecurity deal reached between the US and China, one of the most contentious issue in their

bilateral relations. For years, both sides had accused each other of network infiltration and of stealing confidential information from companies and government agencies. The US had accused China of stealing or compromising a number of weapon systems, such as the F-35 and the PAC3 missile (Meyers, 2015). In 2014, five Chinese hackers were indicted by the Department of Justice over hacking into a number of high-profile companies, such as the United States Steel Corporation (Segal, 2016). China has often responded with counter-claims of being a victim of US intrusions (Singer and Friedman, 2014, p. 189). The agreement struck between President Barack Obama and President Xi Jinping foresees cooperation and mutual assistance in investigations on cybercrime, while both sides committed to restrain from cyber-enabled economic espionage. A monitoring mechanism was established to ensure the proper implementation of this agreement, and a hotline was created to deal with the escalation of issues in cyberspace (White House, 2015).

In this article, we aim to discuss the role of diplomats and diplomacy in addressing cyber issues, which in spite of its rising importance has remained a peripheral issue in the International Relations (IR) literature. More specifically, we seek to understand when and why ministries of foreign affairs (MFAs) started to work on these issues, and how they adapted to a new policy domain. This comes at a time in which diplomacy is changing in terms of its practices (with the progressive adaptation to new technologies), but also in terms of the areas it covers and actors it deals with (Hocking et al., 2012).[2] Cyber-diplomacy can in that regard be seen as the latest instalment, albeit a particularly important one, in what is the progressively changing role of diplomacy in the digital age.[3]

We frame the evolution of cyber-diplomacy from an English School perspective. While diplomacy has often been treated as a mere "constant" (Sending et al., 2015, p. 3) by International Relations scholars, more interested in analysing the origins of power politics or the evolution of warfare, the English School is a distinct exception in having treated diplomacy as one of the essential features of international society. As a school of thought that has revealed a constant, even if not always coherent (see Neumann, 2002), concern for diplomacy, it offers, in our view, important conceptual tools to successfully address such aims, namely the concepts of international society and world society.

Whereas the former "is about the institutionalization of mutual interest and identity among states and puts creation and maintenance of shared norms, rules and institutions at the centre of IR theory" (Buzan, 2014: p.12), the latter "takes individuals, non-state organizations and ultimately the global population as a whole as the focus of global social identities and arrangements and puts transcendence of the state system at the centre of IR theory" (Buzan, 2014, p. 13).

Taking this school of thought as the starting point for our analysis, this paper argues that cyber-diplomacy sits at the intersection between these two societies.[4]

Although both international society and world society are contested concepts around which much has been written, it is not the purpose of this article to engage in theoretical considerations about the ontological and normative basis of both. In that regard, we follow Ian Clark's summative assessment in which he takes the world society to refer to the "non-state social world that takes a transnational form, and is distinct from the society of states" (Clark, 2007, p. 22). For our discussion, it is mostly important to understand international society and world society as analytical concepts that are simultaneously present in international relations. The continuous shift between these two spheres of international life is not without its consequences as we will discuss in the last part of this article. Before that, however, we will explore the concept of cyber-diplomacy and how it differs from other similar concepts (digital diplomacy, e-diplomacy), as well as how this brave new world is being interpreted by those on the ground, the first generation of cyber-diplomats.

Defining cyber-diplomacy

Diplomacy, understood as the attempt to adjust conflicting interests by negotiation and compromise" (Wight, 1979, p. 89) is, for the English School, at the core of international politics; it is a central institution in the definition and maintenance of international society (Hall, 2006; Neumann, 2002, 2003; Watson, 1982). Indeed, for Hedley Bull, diplomacy is "a custodian of the idea of international society, with a stake in preserving and strengthening it" (2002[1977], p. 176). According to him, there are five main functions to the diplomatic practice: to facilitate communication in world politics, to negotiate agreements, to gather intelligence and information from other countries, to avoid or minimise "friction in international relations" (2002[1977], p. 165) and, finally, to symbolise the existence of a society of states.

One of our key assumptions is that these functions remain unaltered, even though the context, actors and issues of diplomatic work have changed since the writings of Hedley Bull. Diplomacy is no longer an activity solely undertaken by a select group of (mostly) white men elegantly discussing and negotiating the main issues in international politics in cocktail parties and at official receptions. It is not even just about relations between states. It now has to take into account "wider relationships and dialogues, involving such entities as regional and international organisations - be they intergovernmental (IGOs) or non-governmental (NGOs) - multinational firms, sub-national actors, advocacy networks, and influential individuals" (Jönsson and Langhorne, 2004, p. vii). As mentioned by former British Ambassador Tom Fletcher regarding the latter group, entrepreneurs such as Google's chairman Eric Schmidt have a "pulling power" that is hard to match for

any state representative (2016, p. 222). They are, in his view, the "new emperors" (idem). Diplomacy has also progressively extended to new policy areas over the years, entering uncharted political territories such as climate negotiations or, lately, cyber issues.

Cyber-diplomacy can be defined as diplomacy in the cyber domain or, in other words, the use of diplomatic resources and the performance of diplomatic functions to secure national interests with regard to the cyberspace. Such interests are generally identified in national cyberspace or cybersecurity strategies, which often include references to the diplomatic agenda. Predominant issues on the cyber-diplomacy agenda include cybersecurity, cybercrime, confidence-building, internet freedom and internet governance.

Cyber-diplomacy is therefore conducted in all or in part by diplomats, meeting in bilateral formats (such as the US-China dialogue) or in multilateral fora (such as in the UN). Beyond the traditional remit of diplomacy, diplomats also interact with various non-state actors, such as leaders of internet companies (such as Facebook or Google), technology entrepreneurs or civil society organisations. Diplomacy can also involve empowering oppressed voices in other countries through technology (Owen, 2015). While this sets quite a broad reach of activities, it does allow us to firmly situate cyber-diplomacy as an international society institution, even when interacting with world society actors. We exclude from our definition the more technical interactions between line ministries (such as justice, telecoms or economy) or official agencies (such as Computer Emergency Response Teams) from different countries, when diplomats are not involved. This is important as it helps differentiate purely diplomatic activities from those that take place between government departments and agencies of different countries, interactions that in many cases predated diplomatic ones as we further explain below, but whose primary concern is to address technical rather than political issues. We recognise that there is a certain 'grey area' where some of these activities may complement or combine themselves. This 'grey area' leads in practice to some tensions between national stakeholders on issues of competence and representation.[5] However, that observation is not fundamentally unlike what is observed in other policy areas, such as the environment or trade.

There is a tendency to conflate two very different ideas: the use of digital tools by diplomats and foreign ministries, and the diplomacy of cyberspace. Following our definition, this article focuses exclusively on the latter, whereas the former fits within what could be labelled as 'e-diplomacy'. Also called 'digital diplomacy', it refers to the use of new technologies and social media by diplomats, in the context of their traditional activities, including for consular purposes (Hocking and Melissen, 2015; Sandre, 2015; Seib, 2016). According to Tom Fletcher, e-diplomacy was officially born on 4 February 1994 when the then Swedish prime

minister Carl Bildt sent the first diplomatic email to US President Bill Clinton congratulating him for lifting the embargo against Vietnam (2016, p. 28). Much of the debate on new diplomacy has been based on this growing reliance on technology for the fulfilment of diplomatic duties (Copeland, 2015, p. 453). Related to it, some see in the necessary adaptation to these technologies (and rationale behind them) the key factor in guaranteeing the predominance of state power in an increasingly networked world (Hocking and Melissen, 2015; Owen, 2015).

Cyber-diplomacy as we define it in this article is a relatively new concept. The term had been used before, but essentially to describe 'e-diplomacy' activities. In a 2002 book entitled *Cyber diplomacy: managing foreign policy in the twenty first century*, for instance, several scholars reflected already on the impact of the internet and new technologies on the objectives, tools and structures of diplomacy (Potter, 2002). The term has also been used to describe the evolution of public diplomacy activities in the digital age (Kleiner, 2008). These early studies focused mostly on the broader digital transformation, but they did not address the diplomatic processes necessary to deal with the emerging international aspects of cyber issues.

The absence of literature results from the novelty of cyber-diplomacy, whose origins we situate at the turn of the first decade of the twenty-first century, as we further explain in the next section. As more attention was given by practitioners to the foreign policy dimension of the cyber agenda, the first policy-oriented studies appeared, making the case for cyber-diplomacy. One of the earliest such studies, published in 2010 by the EastWest Institute, expressed this new interest in clear terms:

> Because of high levels of cross-border connectivity in the cyber world, new approaches for cybersecurity must factor in the international dimension. Thus, instead of exclusively focusing on cyber defense or cyber war, it is also important to begin to develop cyber diplomacy. Few governments have even thought about the diplomatic dimension of cybersecurity, and they certainly haven't developed diplomatic strategies commensurate with the threat (Gady and Austin 2010, p.1).

Although diplomatic practices have significantly developed since then, the literature has surprisingly remained limited, creating a new gap between practice and theory. There have been numerous articles on cyber policies as developed by specific countries, on relations between certain countries, or on specific aspects of international relations in cyberspace[6]. Studies focusing on the competing visions for internet governance have been quite numerous, for instance[7]. Yet, there has been very limited effort to define or conceptualise cyber-diplomacy, and to

understand how diplomats and foreign offices are taking charge of these relatively new issues. More clarity on the definition and purposes of cyber-diplomacy would be useful to those who practice it, whereas the literature on diplomacy and international politics may benefit from hindsight from a new policy domain.

The emergence of cyber-diplomacy: why, when and how

When considering the emergence of cyber-diplomacy, it is important to first understand the underlying logic of cooperation in this policy domain. Cyberspace cumulates a number of characteristics that frame diplomatic engagement among stakeholders. To begin with, it is a global domain connecting nations and citizens worldwide in a variety of manners, generating interactions and frictions between them. Furthermore, cyberspace is usually considered as a "global common", defined as a "resource domain to which all nations have legal access" (Buck, 1998, p. 6). Cyberspace is then comparable to other global commons such as the high seas, airspace and outer space. As such, it is considered that a minimum of rules and regulations are required, in order to ensure access to all and avoid conflict, which can only result from diplomatic negotiations. Those international society principles clash with cyberspace's contested nature in which its major powers promote competing visions, interests and values for the cyberspace. Other relevant characteristics of this realm include the difficulty of attribution of cyber-attacks and intrusions, hindering trust among stakeholders; the advantage of offense over defence capacities, favouring aggressive behaviours; or the digital divide between major cyber powers and developing nations, which create global vulnerabilities. Also, unlike in other areas of the international realm, it is problematic for states to rely on deterrence by retaliation when it comes to cyberspace, due to problems with attribution notably, although other forms of deterrence are possible (van der Meer, 2016; Nye 2017). All these characteristics make both international cyber relations and the governance of the cyberspace extremely complex and fragile, but at the same time make diplomacy all the more necessary, particularly with regard (but not limited) to confidence-building mechanisms and the development of international norms and values.

Cooperation in the cyberspace is thus a choice, not a given. For instance, in a 2015 speech to National Security Agency (NSA) employees, Barack Obama referred to tensions with China as a case in which the US could adopt a confrontational stance, "or, alternatively, (...) try to have some basic rules of the road in terms of how we operate" (quoted in Harold *et al*., 2016, p. 12). In *World Order*, Henry Kissinger gives perhaps the clearest reasoning underpinning the rise of cyber-diplomacy, emphasizing that the absence of dialogue and diplomacy would be detrimental to the cyberspace, but also to the broader world order:

> The road to a world order may be long and uncertain, but no meaningful progress can be made if one of the most pervasive elements of

> international life is excluded from serious dialogue. (…) Absent some articulation of limits and agreement on mutual rules of restraint, a crisis situation is likely to arise, even unintentionally; the very concept of international order may be subject to mounting strains (Kissinger, 2014, pp. 345-6).

The logic of diplomacy in cyberspace is indisputable and yet its practice is very new. This is not due to a sudden change in the above-mentioned characteristics, but rather to the evolution of the governing structures of the cyberspace over time. In the early days, internet was essentially unregulated and its governance largely informal. The main stakeholders were not states, but engineers; it was firmly situated within the realm of world society. Over time, governments became more involved and the cyberspace more regulated. International meetings multiplied, giving way to a plethora of new fora on cyber issues where government technical experts from various line ministries convened to discuss a range of cyber issues, from network security to online criminality. Some of these meetings became structured in the context of international organisations, notably the UN, which launched a World Summit on the Information Society (WSIS) in 2003, with delegates from 175 countries participating, as well as within some regional organisations, such as the European Union, the OSCE, the ASEAN Regional Forum, or the Council of Europe. Yet, the multiplication and institutionalization of these meetings, coupled with the broadening and deepening of the cyber agenda inexorably led to more "politicized struggles", which paved the way to cyber-diplomacy (Deibert, 2015).

The diplomats interviewed for this article concurred with this view that cyber-diplomacy emerged from the internationalisation and politicisation of cyber issues. Cyber issues were treated first as purely technical issues, then as external aspects of domestic policies, before they became recognized as a major foreign policy topic. In the words of one interviewee, there was 'no particular big bang' to explain the sudden interest of diplomats for this policy area, but it was rather a 'growing tide' of events, meetings, issues that required a diplomatic response. Putting it differently, the same interviewee insists that 'diplomats eventually had to step in because cyber became a domain of diplomacy. It is not diplomats that made cyber a foreign policy issue; it already was one.'[8]

At the turn of the first decade of the twenty-first century, several major cyber powers published their first cybersecurity strategies, as the cyberspace and infrastructures became increasingly perceived as strategic assets. The US published its *Cyberspace Policy Review* in 2009, the UK released its *Cybersecurity Strategy* the same year, while China published a *White Paper on Internet in China* in 2010. All these documents were mainly focussed on the domestic aspects of cybersecurity, such as developing cyber capabilities, improving government

coordination, or deepening cooperation with the private sector. The international dimension of cyber issues was addressed, but only marginally (one page or less in the documents mentioned above), to emphasize the need to work with international partners, without much specification.

Several other significant developments marked that period, showing a growing interest of states for cyber issues, and particularly cyber-security, and opportunities for diplomatic engagement. This was notably the case of the successive UN Group of Governmental Experts (UN GGE) meetings, which expressed willingness for the first time in 2010 to work together to reduce the threat resulting from cyber-attacks, and to work towards a set of voluntary norms of responsible State behaviour in the cyberspace. This group was set up following a UN General Assembly Resolution (66/24) proposed by Russia in 2011 (Meyer, 2015, pp. 55-58). It has become a space for the major powers to try to find some come ground, particularly in terms of the development of confidence-building measures.

The starting point of cyber-diplomacy is arguably to be found in the publication of the US *International Strategy for Cyberspace* in 2011, which is the first government document worldwide to focus entirely on the international aspects of cyber issues. The strategy identifies a number of priorities (economy, network protection, law enforcement, military, internet governance, international development, and internet freedom), while relying on three pillars to pursue these objectives: diplomacy, defence and development (3Ds). For the first time, a strategy made a clear case for the use of diplomatic tools and resources in pursuit of cyber-related objectives. In line with the strategy, a new Office of the Coordinator for Cyber Issues was established within the US State Department, becoming the first fully dedicated office to cyber issues in a foreign office worldwide, while the Coordinator Christopher Painter became de facto the world's first cyber-diplomat. This new office was assigned five key tasks (US State Department website, 2017):

- Coordinating the Department's global diplomatic engagement on cyber issues
- Serving as the Department's liaison to the White House and federal departments and agencies on these issues
- Advising the Secretary and Deputy Secretaries on cyber issues and engagements
- Acting as liaison to public and private sector entities on cyber issues
- Coordinating the work of regional and functional bureaus within the Department engaged in these areas

Whereas a growing number of nations have now adopted cybersecurity strategies addressing the international ramifications of cyber issues, only few countries have adopted stand-alone international strategies, similarly to the US. Among the

exceptions, we can point out Japan's *International Strategy on Cybersecurity Cooperation* adopted in 2013, the European Union's member states adopted *Council Conclusions on Cyber Diplomacy* in 2015 – the first time the term 'cyber-diplomacy' was used as such in an official government document – while the 2016 Australian Cybersecurity Strategy committed to establish an *International Engagement Strategy*.

Following the US impetus, other governments created special units for dealing with cyber issues in their MFAs – in some cases prior the adoption of a cybersecurity strategy (e.g. Germany or the EU), in some cases afterwards (e.g. Belgium). The institutional logic of this evolution was that too many departments and desks were dealing simultaneously with cyber issues, without coordination and overarching direction. Furthermore, as pointed out by one interviewee, the creation of a focal point within the MFA was seen as a manner to avoid fragmented reporting from the embassies abroad on cyber-related matters, and therefore to gain a more comprehensive view of the cyber developments and dynamics.[9] In the case of Germany, for instance, the foreign ministry identified no less than 12 different departments involved while it was drafting its cybersecurity strategy in 2010-11. [10] So far, we can identify two main approaches to institutional streamlining in MFAs: either the creation of a new department centralising all cyber-related activities, similarly to other thematic departments; or the establishment of a coordination unit, based on the principle that cyber issues are cross-cutting. Whereas the UK opted for the first option, for instance, the US chose the latter. Hybrid models are possible as well: Germany started by appointing a coordinator, whose work focused initially more on internet freedom and internet governance; but that position evolved into becoming a separate department, as the agenda included more issues related to international cybersecurity and cyber capacity building, while maintaining a coordinating authority over anyone dealing with cyber or internet issues, which is in the words of one interviewee 'a bit of an odd set-up'. [11] Such institutional experimenting certainly has to do with the novelty of cyber issues in contemporary foreign policy, as well as with their cross-cutting nature.

The first diplomats to be appointed with a cyber mandate were really 'pioneers'.[12] They often had to carve a mandate and institutional set-up for themselves. They were also alone in their position originally although in major MFAs they are now teams of a handful people, traditionally including someone at the level of Ambassador, supported by several diplomats and/or officers.

From all these trends emerges the clear notion of a structure very much under construction. As cyberspace is becoming yet another contested area, diplomacy is called upon to fulfil its most traditional functions, including maintaining peace and building mutual confidence between stakeholders, in a completely new

environment – the digital space. A new domain is thus opening up for diplomats, although it is still unclear how much they will succeed in shaping it.

Conclusion: Towards the construction of a cyber-international society?

As established earlier in this article, the activities of cyber-diplomacy shift significantly between international and world societies. More importantly, they operate with concepts, technologies and practices that more often than not were defined within the realm of the latter. It is now, in this concluding section, important to return to this discussion in order to sediment the definition of cyber-diplomacy.

In the last few decades there has been, following Barry Buzan (2014, p. 165-166) a marked tendency to increase the level of interaction between international society and world society as "People everywhere now understand that they are embedded in a single global economy (like it or not), and up to a point that they are also embedded in a single global culture and a single global environment (again, like it or not)." Although, "[t]here isn't a ready-made cosmopolitan alternative to the states-system", Buzan believes "there is increasing interplay and in some ways merger between the different pluralisms in the interstate and world society domains" (2015, p. 166). Indeed, many of the norms that regulate and give legitimacy to international society developed from world society (Clark, 2007, p. 13).

Cyberspace activities have mostly been conducted following a world society rationale best captured by the so-called multi-stakeholder model governing the internet, although states are now trying to come to terms with the importance of the field by incorporating it into the international society realm. All this, without excluding the realist international system, the sphere in which states co-exist and interact without a concern for shared values or norms. Whereas cases such as the July 2016 DNC hacking evidence that state activity in cyberspace is still very much determined by strategic (rather than normative) considerations (realm of the international system), it is the aim of cyber-diplomacy to progressively shift those behaviours and attitudes towards a space of peaceful co-existence, defined by clear rules and principles: from a system of interactive units to a society of states. In that regard, cyber-diplomacy is to cyberspace what diplomacy is to international relations: a fundamental pillar of international society.

Unlike other areas of international life, cyberspace is constituted by a rather incipient set of binding normative arrangements and there is an overall consensus from the diplomats interviewed for this article that much needs to be done in this realm. In the words of one of the interviewees, "in practical terms, at the moment the cyber-world still needs work to ensure adherence to international law and norms of responsible behaviour – otherwise it's pure anarchy".[13] For instance,

whereas armed forces around the world are developing their own cyber-capabilities, there are no "parallel diplomatic processes to develop the agreed parameters for such operations" (Meyer, 2012, p. 16), although work is being done in multiple international fora.

Less than a decade ago, diplomats were called upon to regulate the cyberspace, which had until then escaped the realm of diplomacy. In 2013, the Head of the EU external cyber coordination was observing that 'there are very few nations where national cyber coordination is efficient and the state is able to speak with one voice in all international fora' (Tiirmaa-Klaar, 2013, p. 516). A few years later, things have evolved with a growing number of cyber-diplomats – proudly identified as such on their business cards – engaging bilaterally and multilaterally worldwide.

This article has sought first and foremost to cement the definition of cyber-diplomacy, which we consider a pre-requisite for the development of a coherent body of literature on this topic. We have also sought to explain when and why this practice emerged, again because we consider that a common understanding of the genesis of cyber-diplomacy is necessary to properly conceptualize it. Finally, our article is a plea – or at least an invitation – to the academic community, to look more deeply and systematically into this new practice. The web of cyber-diplomacy is broadening and deepening at a fast pace, progressively creating a cyber-international society. Theory (and academics) must now keep pace with practice.

References

Betz, D. J. & Stevens, T. (2011). *Cyberspace and the state. Toward a strategy for cyber-power*. London: Routledge.

Buck, S.J. (1998). *The global commons: an introduction*. Washington DC: Island Press.

Bull, H. (2002 [1977]). *The Anarchical Society. A Study of Order in World Politics*. 3rd Edition. Basingstoke: Palgrave.

Buzan, B. (2014). *An introduction to the English school of international relations: the societal approach*. Cambridge: Polity Press.

Carr, M. (2017). Cyberspace and International Order. In Suganami, H., Carr, M. & Humphreys, A. (eds.), *The Anarchical Society at 40. Contemporary Challenges & Prospects* (pp. 162-178). Oxford: OUP.

Clark, I. (2007). *International Legitimacy and World Society*. Oxford: OUP.

Copeland, D. (2015). Digital Technology. In Cooper, A.F., Heine, J. & Thakur, R. (eds.) *The Oxford Handbook of Modern Diplomacy* (pp. 453-472). Oxford: OUP.

Deibert, R. (2015). The geopolitics of cyberspace after Snowden. *Current History*, January, 9-15.

Dunne, T. (1998). *Inventing International Society. A History of the English School*. Basingstoke: Macmillan Press Ltd.

Dunn Cavelty, M. (2007). *Cyber-security and threat politics: US efforts to security the information age*. London: Routledge.

Eriksson, J. & Giacomello, G. (eds.). (2010). *International Relations and Security in the Digital Age*, London: Routledge.

Fletcher, T. (2016). *Naked Diplomacy. Power and Statecraft in the Digital Age*. London: William Collins.

Gady, F.S. & Austin, G. (2010). *Russia, the United States and cyber diplomacy: opening the doors*, New York: EastWest Institute.

Hall, I. (2006). Diplomacy, Anti-diplomacy and International Society. In Little, R. & Williams, J. (eds.). *The Institutions of Anarchical Society* (pp. 141-161). Basingstoke: Palgrave Macmillan.

Harold, S.W., Libicki, M.C. & Stuth Cevallos, A. (2016). *Getting to yes with China in cyberspace*. Santa Monica: RAND Corp.

Hocking, B. & Melissen, J. (2015). *Diplomacy in the digital age*. The Hague: Clingendael Institute.

Hocking, B., Melissen, J., Riordan, S. & Sharp, P. (2012). *Futures for diplomacy. Integrative Diplomacy in the 21st century*. The Hague: Clingendael Institute.

Horten, M. (2016). *The Closing of the Net*. Cambridge: Polity.

Jönsson, C. & Langhorne, R. (2004). Editor's Introduction. In Jönsson, C. & Langhorne, R. (eds). *Diplomacy. Volume III. Problems and Issues in Contemporary Diplomacy* (pp. vii-xiii). London: Sage Publications.

Kello, L. (2013). The Meaning of the Cyber Revolution. *International Security*, 38(2), 7-40.

Kissinger, H. (2014). *World Order*. New York: Penguin Press.

Kleiner, J. (2008). The Inertia of Diplomacy. *Diplomacy & Statecraft*, 19(2), 321-349.

Meyer, P. (2012). Diplomatic Alternatives to Cyber-Warfare. *The RUSI Journal*, 157(1), 14-19.

Meyer, P. (2015). Seizing the Diplomatic Initiative to Control Cyber Conflict. *The Washington Quarterly*, 38(2), 47-61.

Mueller, M. (2017). *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*. Cambridge: Polity Press.

Neumann, I. (2002). *The English School on Diplomacy* (*Clingendael Discussion Paper* 79). The Hague: Clingendael Institute

Nye Jr, J.S. (2017). Deterrence and dissuasion in cyberspace. *International Security*, 41(3), 44–71.

Owen, T. (2015). *Disruptive Power: The Crisis of the State in the Digital Age*. Oxford: OUP.

Potter, E.H. (2002). *Cyber-diplomacy: Managing Foreign Policy in the Twenty-first Century*. Montreal: McGill-Queen's University Press.

Pouliot, V. & Cornut, J. (2015). Practice theory and the study of diplomacy: A research agenda. *Cooperation and Conflict*, 50(3), 297-315.

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, 35(1), 5-32.

Sandre, A. (2015). *Digital Diplomacy. Conversations on Innovation in Foreign Policy*. Lanham: Rowman&Littlefield.

Adam Segal (2016) *The Hacked World Order How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, Philadelphia: Public Affairs.

Seib, P. (2016). *The Future of Diplomacy*. Cambridge: Polity.

Sending, O.J., Pouliot, V. & Neumann, I.B. (2015). Introduction. In Sending, O.S., Pouliot, V. & Neumann, I.B. (eds.). *Diplomacy and the Making of World Politics* (pp. 1-28). Cambridge: CUP.

Singer, P. & Friedman, A. (2014). *Cybersecurity and Cyberwar. What Everyone Needs to Know*. Oxford: Oxford University Press.

State Council of China. (2010). *White Paper on the Internet in China*. Beijing: Information Office of the State Council of the People's Republic of China.

Tiirmaa-Klaar, H. (2013). Cyber diplomacy: agenda, challenges and mission. In Ziolkowski, K. (ed). *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (pp. 509-31). Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

UK Prime Minister. (2009). *Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space*. London: Office of the UK Prime Minister.

Office of the Coordinator for Cyber Issues: https://www.state.gov/s/cyberissues/, accessed on 20 February 2017.

Watson, A. (1982). *Diplomacy. The Dialogue Between States*. London: Routledge.

Wight, M. (1979). *Systems of States*. Leicester: Leicester University Press.

White House. (2009). *Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure*. Washington DC: The White House.

White House. (2011). *International strategy for cyberspace*. Washington DC: The White House.

White House. (2015). *FACT SHEET: President Xi Jinping's State Visit to the United States*. Washington DC: The White House Office of the Press Secretary, 25 September.

Van der Meer, S. (2016). Enhancing International Cyber Security. A Key Role for Diplomacy. *Security and Human Rights*, 26, 193-205.

[1] The authors would like to thank all the anonymous diplomats who have agreed to meet and discuss these issues with us, as well as the editors and reviewers of *Global Affairs* for their relevant insights. The usual disclaimer applies.

[2] Here we follow Pouliot and Cornut when they argue: "[p]ractices are ways of doing things. Seen through these lenses, diplomacy as a bundle of practices is a fundamentally dynamic process. It is not an outcome, but an activity" (2015, p. 300). For a discussion on the relation between practices and the English School, see Navari, 2010.

[3] In the literature, the words 'digital' and 'cyber' are often used interchangeably, although the latter has often more of a security connotation, whereas the former connotes more technological and economic aspects (the expression 'digital age' in our title refers to our societies' growing reliance on digital tools and technologies). In this article, we distinguish 'cyber' from 'digital' diplomacy, notably on that basis. Another reason to prefer the prefix 'cyber' throughout this article is to reflect the diplomats' own vocabulary.

[4] For a different application of the English School to cyberspace – the application of Hedley Bull's thought to attribution in cyberspace – see Carr (2017).

[5] Interview, German diplomat, by telephone, 26 January 2017.

[6] Myriam Dunn Cavelty (2007), Thomas Rid (2012; 2013), and Peter W. Singer and Allan Friedman (2014) provide some excellent discussion on cyber war and cyber security. More broadly, Lucas Kello (2013), Madeline Carr (2017), David Betz and Tim Stevens (2011), Erikson and Giacomello (2010), and Adam Segal (2016) address the implications of cyberspace for international relations.

[7] On internet governance, see Horten (2016) and Mueller (2017).

[8] Interview, German diplomat, 20 January 2017.

[9] Interview, Belgian diplomat, Brussels, 10 January 2017.

[10] Interview, German diplomat, 20 January 2017.

[11] Interview, German diplomat, by telephone, 26 January 2017.

[12] Interview, German diplomat, by telephone, 26 January 2017.

[13] Interview, German diplomat, by telephone, 26 January 2017.